Draft (2nd) NISTIR 8259

Recommendations for IoT Device Manufacturers:

Foundational Activities and Core Device Cybersecurity Capability Baseline

Michael Fagan
Katerina N. Megas
Karen Scarfone
Matthew Smith

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8259-draft2

National Institute of
Standards and Technology
U.S. Department of Commerce

Draft (2nd) NISTIR 8259

Recommendations for IoT Device Manufacturers:

Foundational Activities and Core Device Cybersecurity Capability Baseline

Michael Fagan
Katerina N. Megas
Applied Cybersecurity Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

Matthew Smith
G2, Inc.
Annapolis Junction, MD

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8259-draft2

January 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8259
41 pages (January 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8259-draft2

Public comment period: ***January 7, 2020 through February 7, 2020***

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: iotsecurity@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

Internet of Things (IoT) devices often lack device cybersecurity capabilities their customers—organizations and individuals—can use to help mitigate their cybersecurity risks. Manufacturers can help their customers by improving how securable the IoT devices they make are, meaning the devices provide functionality that their customers need to secure them within their systems and environments, and manufacturers can also help their customers by providing them with the cybersecurity-related information they need. This publication describes voluntary, recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers. These activities can help manufacturers lessen the cybersecurity-related efforts needed by IoT device customers, which in turn can reduce the prevalence and severity of IoT device compromises and the attacks performed using compromised IoT devices.

Keywords

cybersecurity baseline; cybersecurity risk; Internet of Things (IoT); manufacturing; risk management; risk mitigation; securable computing devices; software development

Acknowledgments

The authors wish to thank all contributors to this publication, including the participants in workshops and other interactive sessions; the individuals and organizations from the public and private sectors, including manufacturers from various sectors as well as several manufacturer trade organizations, who provided feedback on the preliminary essay and the initial public comment draft; and colleagues at NIST who offered invaluable inputs and feedback.

Audience

The main audience for this publication is IoT device manufacturers. This publication may also help IoT device customers that use IoT devices and want to better understand what device cybersecurity capabilities they may offer and what cybersecurity information their manufacturers may provide.

Note to Reviewers

Reviewers of the first public comment draft of this publication will notice many changes to the structure of the publication. The main concepts within the publication remain the same; it is only their presentation that has been revised to clarify the concepts and address other comments from the public. NIST encourages reviewers of the first public comment draft to read this full draft and provide comments on any areas where additional clarity may be needed.

Trademark Information

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: iotsecurity@nist.gov

Executive Summary

Manufacturers are creating an incredible variety and volume of internet-ready devices broadly known as the Internet of Things (IoT). Most of these IoT devices do not fit the standard definitions of information technology (IT) devices that have been used as the basis for defining device cybersecurity capabilities (e.g., smartphones, servers, laptops). The IoT devices in scope for this publication have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution [LTE], Zigbee, Ultra-Wideband [UWB]) for interfacing with the digital world. Many IoT devices provide computing functionality, data storage, and network connectivity for equipment that previously lacked these functions. In turn, these functions enable new efficiencies and technological capabilities for the equipment, such as remote access for monitoring, configuration, and troubleshooting. IoT can also add the ability to analyze data about the physical world and use the results to better inform decision making, alter the physical environment, and anticipate future events. [1]

IoT devices are acquired and used by many customers: individuals, companies, government agencies, educational institutions, and other organizations. Unfortunately, IoT devices often lack device capabilities customers can use to help mitigate their cybersecurity risks. Consequently, IoT device customers may have to select, implement, and manage additional or new cybersecurity controls or alter the controls they already have. Compounding this, customers may not know they need to alter their existing processes to accommodate IoT. The result is many IoT devices are not secured in the face of evolving threats; therefore, attackers can more easily compromise IoT devices and use them to harm device customers and conduct additional nefarious acts (e.g., distributed denial of service [DDoS] attacks) against other organizations.[1]

Manufacturers can help their customers address the challenges of IoT cybersecurity by improving how securable the IoT devices they make are, meaning the devices provide capabilities that device customers—both organizations and individuals—need to secure them within their systems and environments, and manufacturers provide their customers with the cybersecurity-related information they need.

This document describes six voluntary, but recommended activities related to cybersecurity that manufacturers should consider performing before their IoT devices are sold to customers. Four of the six activities primarily impact decisions and actions performed by the manufacturer before a device is sent out for sale (pre-market), and the remaining two activities primarily impact decisions and actions performed by the manufacturer after device sale (post-market). Performing all six activities can help manufacturers provide IoT devices that better support the cybersecurity-related efforts needed by IoT device customers, which in turn can reduce the

[1] In 2017, Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [2], was issued to improve the Nation's cyber posture and capabilities in the face of intensifying threats. The Executive Order tasked the Department of Commerce and Department of Homeland Security with creating the Enhancing Resilience Against Botnets Report [3] to determine how to stop attacker use of botnets to perform DDoS attacks. This report contained many action items, and this document fulfills two of them: to create a baseline of cybersecurity capabilities for IoT devices, and to publish cybersecurity practices for IoT device manufacturers.

prevalence and severity of IoT device compromises and the attacks performed using compromised IoT devices.

Activities with Primarily Pre-Market Impact

- **Activity 1: Identify expected customers and define expected use cases.** Identifying the expected customers and use cases for an IoT device early in its design is vital for determining which device cybersecurity capabilities the device should implement and how it should implement them.
- **Activity 2: Research customer cybersecurity goals.** Manufacturers cannot completely understand all of their customers' risk because every customer faces unique risks based on many factors. However, manufacturers can make their devices at least minimally securable by those they expect to be customers of their product who use them consistent with the expected use cases.
- **Activity 3: Determine how to address customer goals.** Manufacturers can determine how to address those goals by having their IoT devices provide particular device cybersecurity capabilities in order to help customers mitigate their cybersecurity risks. To provide manufacturers a starting point to use in identifying the necessary device cybersecurity capabilities, this document defines a core device cybersecurity capability baseline, which is a set of device cybersecurity capabilities that customers are likely to need:
    - **Device Identification**: The IoT device can be uniquely identified logically and physically.
    - **Device Configuration**: The configuration of the IoT device's software and firmware can be changed, and such changes can be performed by authorized entities only.
    - **Data Protection**: The IoT device can protect the data it stores and transmits from unauthorized access and modification.
    - **Logical Access to Interfaces**: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.
    - **Software and Firmware Update**: The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.
    - **Cybersecurity State Awareness**: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.
- **Activity 4: Plan for adequate support of customer goals.** Manufacturers can help make their IoT devices more securable by appropriately provisioning device hardware, firmware, software, and business resources to support the desired device cybersecurity capabilities.

Activities with Primarily Post-Market Impact

- **Activity 5: Define approaches for communicating to customers.** Many customers will benefit from manufacturers communicating to them—or others acting on the customers' behalf, such as an internet service provider or a managed security services provider—more clearly about cybersecurity risks involving the IoT devices the manufacturers are currently selling or have already sold.

- **Activity 6: Decide what to communicate to customers and how to communicate it.** There are many potential considerations for what information a manufacturer communicates to customers for a particular IoT product and how that information will be communicated. Examples of topics are:
    - Cybersecurity risk-related assumptions that the manufacturer made when designing and developing the device
    - Support and lifespan expectations
    - Device cybersecurity capabilities that the device provides, as well as cybersecurity functions that can be provided by a related device or a manufacturer service or system
    - Device composition and capabilities, such as information about the device's software, firmware, hardware, services, functions, and data types
    - Software and firmware updates
    - Device retirement options

Table of Contents

List of Appendices

1 Introduction

1.1 Purpose and Scope

The purpose of this publication is to give manufacturers voluntary recommendations for improving how *securable* the IoT devices they make are. This means the IoT devices offer *device cybersecurity capabilities*—cybersecurity features or functions the devices provide through their own technical means (i.e., device hardware, firmware, and software)—that device customers, both organizations and individuals, need to secure them within their systems and environments. From this publication, IoT device manufacturers will learn how they can help IoT device customers with cybersecurity risk management by carefully considering which device cybersecurity capabilities to design into their devices for customers to use in managing their cybersecurity risk.

The publication is intended to address a wide range of IoT devices. The IoT devices in scope for this publication have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution [LTE], Zigbee, Ultra-Wideband [UWB]) for interfacing with the digital world. The IoT devices in scope for this publication can function on their own and are not only able to function when acting as a component of another device, such as a processor. Some IoT devices may be dependent on specific other devices (e.g., a hub) or systems (e.g., a cloud) for some functionality. Also, no IoT device operates in isolation. Rather, IoT devices will be used in systems and environments with many other devices and components, some of which may be IoT devices, while others may be conventional IT equipment. All parts of the IoT ecosystem other than the IoT devices themselves are outside the scope of this publication.

This document is intended to inform the manufacturing of new devices and not devices that are already in production, although some of the information in this publication might also be applicable to such devices.

Readers do not need a technical understanding of IoT device composition and capabilities, but a basic understanding of cybersecurity principles is assumed.

1.2 Publication Structure

The remainder of this publication is organized into the following sections and appendices:

- Section 2 provides background on how manufacturers can affect how securable their IoT devices are for their customers, such as which cybersecurity risk mitigation areas customers commonly need to address.
- Sections 3 and 4 describe activities manufacturers should consider performing before their IoT devices are sold to customers in order to improve how securable the IoT devices are for the customers.
    - Section 3 includes activities that primarily impact other activities performed by the manufacturer before device sale. The Section 3 activities are: identifying expected customers and defining expected use cases, researching customer

cybersecurity goals, determining how to address customer goals, and planning for adequate support of customer goals.

  - Section 4 includes activities that primarily impact other activities performed by the manufacturer after device sale. The Section 4 activities are: defining approaches for communicating with customers regarding IoT device cybersecurity, and deciding what to communicate to customers and how to communicate it.

- Section 5 provides a conclusion for the publication that explores next steps for manufacturers or other stakeholders in the IoT ecosystem.
- The References section lists the references for the publication.
- Appendix A provides an acronym and abbreviation list.
- Appendix B contains a glossary of selected terms used in the publication.

2 Background

From a manufacturer's perspective, the *pre-market* phase of an IoT device's life encompasses what the manufacturer does *before* the device is marketed and sold to a customer. Any actions the manufacturer takes for an IoT device after it is sold, such as addressing vulnerabilities, delivering updated or new device capabilities, or providing cybersecurity information to customers, are considered part of the *post-market* phase. Manufacturers are generally best able to identify and incorporate plans for the device cybersecurity capabilities their devices will support early in the pre-market phase. Later in the pre-market phase, making design or implementation changes is usually more complicated and costly, and might necessitate delaying the release of the device. Once a device is on the market, many cybersecurity changes may no longer be viable, especially if they necessitate changes to hardware, and those that can still be accomplished may be much more costly and difficult than if they had been done pre-market.

Sections 3 and 4 of this document describe cybersecurity activities and related planning that manufacturers should consider performing during the pre-market phase for an IoT device. Section 3 covers activities that primarily impact other pre-market activities, while Section 4 discusses activities that primarily impact post-market activities. The activities in Sections 3 and 4 focus on key cybersecurity activities and only represent a subset of what manufacturers may need to do during their product development process and are not intended to be comprehensive. For example, manufacturers will also find it easier to design and produce securable IoT devices if they ensure their workforce has the necessary skills to perform the activities in Sections 3 and 4 before starting to perform them.

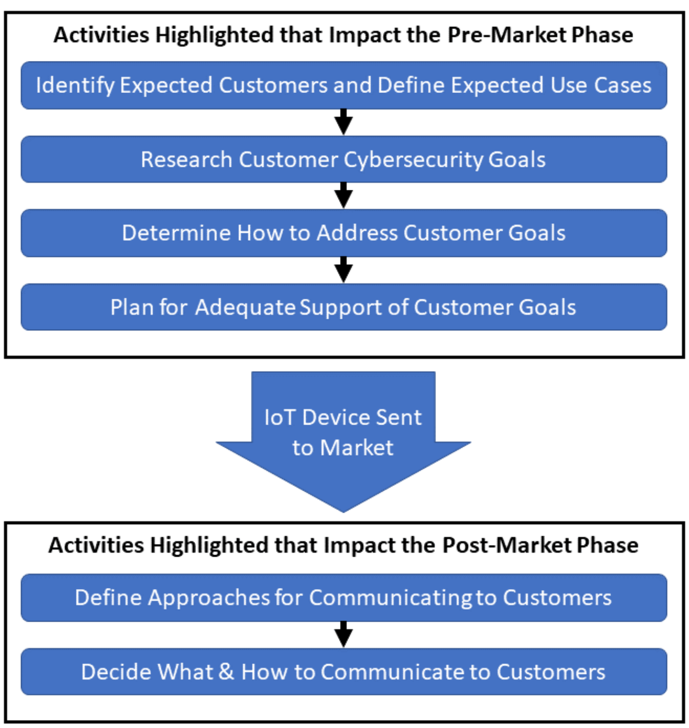

Figure 1: Activities Discussed in this Document Grouped by Phase Impacted

Figure 1 shows the activities covered in this document, arranged by the phase in which the outcomes of the activities will be used to increase device securability. As indicated in the figure, activities highlighted for each phase build on each other within that phase such that each pre-market activity will build on the outcomes of prior activities. While highlighted activities impacting the post-market phase may use artifacts and outcomes from pre-market activities, they may also draw on other sources of guidance and information. The moment at which a device is considered to have "gone to market" will vary by product, manufacturer, and circumstance, but is defined as when a manufactured device is no longer under the control of the manufacturer (i.e., when it has been released to an intermediary, such as a retailer, or an end-customer). Activities primarily impacting the post-market phase, though intended to help the securability of IoT devices after or as they are sold (e.g., by helping inform customers how a device can help meet their cybersecurity goals), should be planned to start in the pre-market phase.

Improving how securable an IoT device is for customers means helping customers meet their risk mitigation goals, which involves addressing a set of risk mitigation areas. Even customers without formal risk mitigation goals, such as home consumers, often have informal and indirect goals, like having their IoT device provide the desired functionality as expected, that are dependent to some extent on addressing risk mitigation areas. Based on an analysis of existing NIST publications such as the Cybersecurity Framework [6] and SP 800-53 [5] and the characteristics of IoT devices, NIST IR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [4] identified the common risk mitigation areas for IoT devices as:

- **Asset Management:** Maintain a current, accurate inventory of all IoT devices and their relevant characteristics throughout the devices' lifecycles in order to use that information for cybersecurity risk management purposes. Being able to distinguish each IoT device from all others is needed for the other common risk mitigation areas—vulnerability management, access management, data protection, and incident detection.
- **Vulnerability Management:** Identify and eliminate known vulnerabilities in IoT device software and firmware throughout the devices' lifecycles in order to reduce the likelihood and ease of exploitation and compromise. Vulnerabilities can be eliminated by installing updates (e.g., patches) and changing configuration settings. Updates can also correct IoT device operational problems, which can improve device availability, reliability, performance, and other aspects of device operation. Customers often want to alter a device's configuration settings for a variety of reasons, including cybersecurity, interoperability, privacy, and usability.
- **Access Management:** Prevent unauthorized and improper physical and logical access to, usage of, and administration of IoT devices throughout the devices' lifecycles by people, processes, and other computing devices. Limiting access to interfaces reduces the attack surface of the device, giving attackers fewer opportunities to compromise it.
- **Data Protection:** Prevent access to and tampering with data at rest or in transit that might expose sensitive information or allow manipulation or disruption of IoT device operations throughout the devices' lifecycles.
- **Incident Detection:** Monitor and analyze IoT device activity for signs of incidents involving device and data security throughout the devices' lifecycles. These signs can

also be useful in investigating compromises and troubleshooting certain operational problems.

Manufacturers of IoT devices addressing these areas by incorporating corresponding device cybersecurity capabilities into their IoT devices will help reduce customer challenges in securing those devices by aligning IoT device capabilities better with customer expectations. Many of these areas can only be addressed effectively, and most are addressed more efficiently, by device cybersecurity capabilities being built into devices instead of customers providing them through their environments.

Sections 3 and 4 of NIST IR 8228 [4] discuss additional cybersecurity-related considerations that manufacturers should be mindful of when identifying the device cybersecurity capabilities IoT devices provide. Also, Tables 1 and 2 in Section 4 of NIST IR 8228 list common shortcomings in IoT device cybersecurity, explain how they can negatively impact customers, and provide the rationales for needing each capability and key element in the core baseline in this document.

For many IoT devices, additional types of risks, such as privacy,[2] safety, reliability, or resiliency, need to be managed simultaneously with cybersecurity risks because of the effects addressing one type of risk can have on others. A common example is ensuring that when a device fails, it does so in a safe manner. Only cybersecurity risks are discussed in this publication. Readers who are interested in better understanding other types of risks and their relationship to cybersecurity may benefit from reading NIST SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security* [7] and NIST SP 1500-201, *Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0* from the Cyber-Physical Systems Public Working Group [8].

[2] A number of privacy efforts, including the NIST Privacy Framework (https://www.nist.gov/privacy-framework), are currently underway that are likely to inform needed IoT device capabilities to support privacy. While the core baseline includes device cybersecurity capabilities that also support privacy, such as protecting the confidentiality of data, it does not include non-cybersecurity related device capabilities that support privacy.

3 Manufacturer Activities Impacting the IoT Device Pre-Market Phase

Manufacturers should consider performing the activities described in this section in order to improve how securable the IoT device is for customers (e.g., increase the number or efficacy of customer-expected device cybersecurity capabilities offered on IoT devices). The activities are meant to be conducted in parallel with or as extensions of a manufacturer's other pre-market activities, and they will primarily impact those other pre-market activities. Some of these activities can have broader purposes than cybersecurity (e.g., exploring expected customers and use cases); effort should not be duplicated, and artifacts from all pre-market activities can inform cybersecurity-specific actions. The more integrated these suggested activities are with other pre-market activities, the better cybersecurity is likely to be planned for and implemented in IoT devices.

3.1 Activity 1: Identify Expected Customers and Define Expected Use Cases

Identifying the expected customers for an IoT device early in its design is vital for determining which device cybersecurity capabilities the device should implement and how it should implement them. For example, a large company might need a device to integrate with its log management servers, but a typical home customer would not. Manufacturers can answer questions like the following:

1. **Which types of people are expected customers for this device?** (e.g., musicians, small business owners, cyclists, police officers, chefs, home builders, preschoolers, electrical engineers)
2. **Which types of organizations are expected customers for this device?** (e.g., small retail businesses, large hospitals, energy companies with solar farms, educational institutions with buses)

Another early step in IoT device design is defining expected use cases for the device based on the expected customers. To help define a use case, manufacturers can answer the following questions, based on how they anticipate the device will be reasonably deployed and used:

1. **How will the device be used?** (e.g., for a single purpose or for multiple purposes; embedded within another device or not embedded)
2. **Where geographically will the device be used?** (e.g., countries, jurisdictions within countries)
3. **What physical environments will the device be used in?** (e.g., inside or outside; stationary or moving; public or private; movable or immovable)
4. **What dependencies on other systems will the device likely have?** (e.g., requires use of a particular IoT hub; uses cloud-based third-party services for some functionality)
5. **How might attackers misuse and compromise the device within the context of the use case?** (i.e., potential pairings of threats and vulnerabilities, such as in a threat model)
6. **What other aspects of device use might be relevant to the device's cybersecurity risk?**

3.2 Activity 2: Research Customer Cybersecurity Goals

Manufacturers cannot completely understand all of their customers' risk because every customer, system, and IoT device faces unique risks based on many factors. However, manufacturers can consider the expected use cases for their IoT devices, then make their devices at least minimally securable by customers who acquire and use them consistent with those use cases. *Minimally securable* means the devices have the device cybersecurity capabilities customers may need to mitigate some common cybersecurity risks. Customers also have a role in securing their IoT devices and the systems that incorporate those devices, including using additional technical, physical, and procedural means. The degree to which a customer may have a role will vary, but for most customers and use cases, device cybersecurity capabilities built into IoT devices generally make risk mitigation easier and more effective for customers.

Customers will use *means* to achieve their goals. *Means* is defined as "an agent, tool, device, measure, plan, or policy for accomplishing or furthering a purpose." [9] This publication refers to technical or non-technical means for cybersecurity purposes, whether performed by an IoT device itself or elsewhere. The term introduced in Section 1, *device cybersecurity capabilities*, refers to technical means being performed by an IoT device itself.

As Figure 2 demonstrates, the connections between manufacturers and customers around cybersecurity are important to keep in mind. Customers who buy and use IoT devices are intending to connect those devices to systems and networks, including the internet. As customers adopt these devices, they will seek to secure them in order to meet their goals. IoT devices that support the device cybersecurity capabilities customers need or expect will be easier for customers to secure, particularly using mechanisms customers have already implemented. Manufacturers can anticipate many customer cybersecurity goals, especially those based on existing cybersecurity guidance and requirements—for example, customers in a particular sector may be required by regulations to change all default passwords.

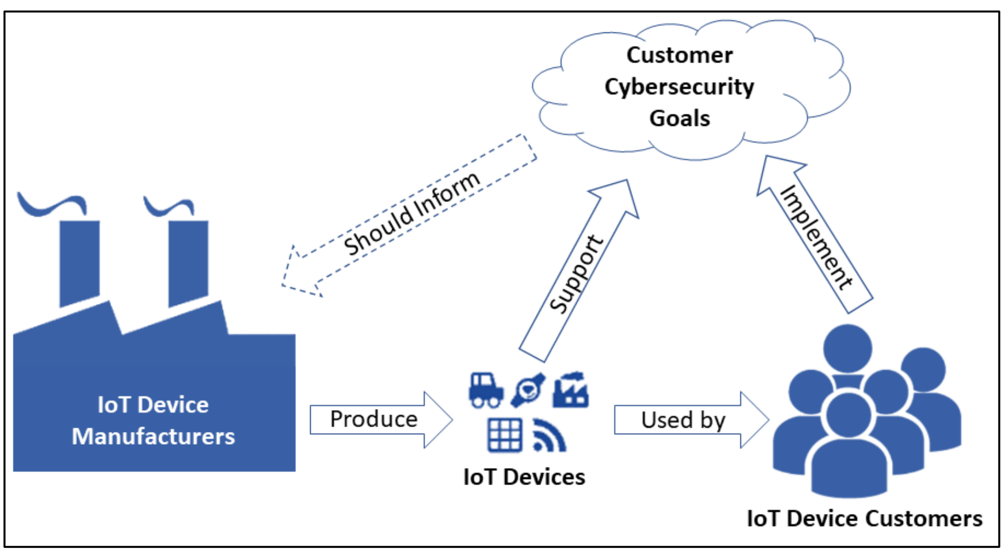

Figure 2: Connections Between IoT Device Manufacturers and Customers Around Cybersecurity

Cybersecurity risks for IoT devices can be thought of in terms of two high-level risk mitigation goals. The first is safeguarding the confidentiality, integrity, and availability of the device itself—to prevent the device from being misused to negatively impact the customer or to attack other organizations, or from not providing the expected functionality for the customer. The second is safeguarding the confidentiality, integrity, and/or availability of data (including personally identifiable information [PII]) collected by, stored on, processed by, or transmitted to or from the IoT device.

To gather information on customer goals related to safeguarding device integrity and data confidentiality, integrity, and availability, manufacturers can answer the following questions for each of the expected use cases:

1. **How will the IoT device interact with the physical world?** The potential impact of some IoT devices making changes to physical systems and thus affecting the physical world needs to be explicitly recognized and addressed from a cybersecurity perspective. Also, operational requirements for performance, reliability, resilience, and safety may be at odds with common cybersecurity practices for conventional IT devices.
2. **How will the IoT device need to be accessed, managed, and monitored by authorized people, processes, and other devices?** Examples include the following:
    - The methods likely to be used by device customers to manage the device are important to consider. An IoT device could support integration with common enterprise systems (e.g., asset management, vulnerability management, log management) to give customers with these systems greater control and visibility into the devices' cybersecurity risk. For an IoT device expected to be used in home environments only, this capability would not be relevant; customers would expect a user-friendly way to manage their devices, or even want the manufacturer to perform all device management on their behalf (e.g., install patches automatically). An IoT device used by a small business might also be managed by a third party on behalf of the business.
    - Making a device highly configurable is generally more desirable in organization environments and less so in home customer settings. A home customer is less likely to understand the significance of granular cybersecurity configuration settings and thus misconfigure a device, weakening its security and increasing the likelihood of a compromise. Some home customers are also unlikely to want to change configuration settings after initial device deployment. However, some configuration settings, such as enabling or disabling clock synchronization services for the device and choosing a time server to use for clock synchronization, may be desired by many customers, including industrial, enterprise, and home customers. Device configuration might be entirely omitted in cases where the device does not need to be provisioned or customized in any way during or after deployment (e.g., does not need to be joined to a wireless network, does not need to be associated with a particular user).
    - Consider how accessible the device is, either logically or physically. Imagine an IoT food vending machine in a public place, which is internet connected so suppliers can track inventory and machine status. Vending machine users would not be required to

authenticate themselves in order to insert money and purchase a snack. However, the vending machine would also be highly susceptible to physical attack.

- Consider allowing device cybersecurity capabilities that may negatively impact operations to be disabled. An example is capabilities intended to deter brute force attacks against passwords, such as locking out an account after too many failed authentication attempts, because these can inadvertently cause a denial of service for the person or device attempting to authenticate. In safety-critical environments, such disruptions to access may not be acceptable because of the danger they would cause. Customers often need flexibility in configuring such features or disabling them altogether.

3. **How will the IoT device's use of device cybersecurity capabilities be affected in terms of the device's availability, efficiency, and effectiveness?** Here is an example. Devices expected to be used on low bandwidth or unreliable networks might not be able to use certain device capabilities. Depending on such a network for downloading large updates might saturate the network connection, disrupting other usage, and take too long to get updates to the device. Manufacturers could consider alternative update strategies, such as changing their processes to reduce update sizes, or distributing updates to administrators on high-speed network connections and having the administrators manually transfer the updates to the IoT device (which introduces additional cybersecurity risks from malware being transmitted by removable media that may need to be mitigated).

4. **What will the nature of the IoT device's data be?** There is a great deal of variability in data across IoT devices; some devices do not store any data, while others store data that could cause significant harm if accessed or modified by unauthorized entities. Understanding the nature of data on a device in the context of the customers and use cases can help manufacturers identify which device cybersecurity capabilities may be needed for protecting device data, such as data encryption, device and user authentication, access control, and backup/restore.

5. **What are the known cybersecurity requirements for the IoT device?** Manufacturers can identify known requirements in their use cases, such as sector-specific cybersecurity regulations or country-specific laws, so they can be mindful of those requirements during device capability identification.

6. **What complexities will be introduced by the IoT device interacting with other devices, systems, and environments?** For example, complexity can be driven by new uses of IoT and IoT devices, new combinations of those devices with each other and conventional IT devices, and increasing interconnections among devices and systems. These complexities could mean new functionality, which may have human-safety or privacy implications, will be connected via networking technologies to systems that do not appropriately mitigate these risks. An IoT device that can stream images from inside the home, such as a smart baby monitor, or that can alter the environment to the point of danger, such as a smart oven, might require safeguards not usually considered for conventional IT devices. IoT can also introduce complexities related to scale, which could make ongoing management and support of devices difficult.

3.3 Activity 3: Determine How to Address Customer Goals

After researching the cybersecurity goals for the IoT device's expected customers and use cases, manufacturers can determine how to address those goals in order to help customers mitigate cybersecurity risks. For each cybersecurity goal, the manufacturer can answer this question: **which one or more of the following is a suitable means (or combination of means) to achieve the goal?**

- The IoT device can provide the technical means through its device cybersecurity capabilities (for example, by using device cybersecurity capabilities built into the device's operating system, or by having the device's application software provide device cybersecurity capabilities).
- Another device related to the IoT device (e.g., an IoT gateway or hub also from the manufacturer, a third-party IoT gateway or hub) can provide the technical means on behalf of the IoT device (e.g., acting as an intermediary between the IoT device and other networks while providing command and control functionality for the IoT device).
- Other systems and services acting on behalf of the manufacturer can provide the technical means (e.g., a cloud-based service that securely stores data for each IoT device).
- The customer can select and implement other technical and non-technical means for mitigating cybersecurity risk. (The customer can also choose to respond to cybersecurity risk in other ways, including accepting or transferring it.) For example, an IoT device may be intended for use in a customer facility with stringent physical security controls in place.

Note that there is not necessarily a one-to-one correspondence between goals and technical means; for example, it may take multiple technical means to achieve a goal, and a single technical means may help address multiple goals.

In addition to identifying suitable means for addressing each cybersecurity goal, manufacturers can also answer this question: **how robustly must each technical means be implemented in order to achieve the cybersecurity goal?** Here are some examples of potential robustness considerations:

- Whether it needs to be implemented in hardware or can be implemented in software instead
- Which data needs to be protected, what types of protection each instance of data needs (e.g., confidentiality, integrity), and how strong that protection needs to be
- How strongly an entity's identity needs to be authenticated before granting access (e.g., PIN, password, passphrase, two-factor authentication)
- How readily software and firmware updates can be reverted if a problem occurs (e.g., a rollback capability, an anti-rollback capability)

Ultimately, manufacturers can aggregate the technical means identified for all the goals to answer the following question: **which technical means will be provided by the IoT device itself, other devices related to the IoT device, other systems and services acting on behalf of**

the manufacturer, and the customer, and how robust should each of those means be? The rest of this publication focuses on the first part of the question: which technical means will be provided by the IoT device itself—in other words, device cybersecurity capabilities?

Identifying the device cybersecurity capabilities that the device itself needs to provide should happen as early as feasible in device design processes so the capabilities can be taken into account when selecting or designing IoT device hardware, firmware, and software. To provide manufacturers a starting point to use in identifying the necessary device cybersecurity capabilities for their IoT devices, Table 1 defines a core device cybersecurity capability baseline (*core baseline*),[3] which is a set of device capabilities generally needed to support common cybersecurity controls that protect the customer's devices and device data, systems, and ecosystems. The core baseline has been derived from common cybersecurity risk management approaches. The risk mitigation areas that are supported by each device capability in Table 1 are shown in Figure 2 after the table to indicate how these capabilities are intended to support common cybersecurity controls.

The core baseline's role is as a default for minimally securable devices, meaning that device cybersecurity capabilities will often need to be added or removed from an IoT device's design to take into account the manufacturer's understanding of customers' likely cybersecurity risks. The core baseline does not specify how the device cybersecurity capabilities are to be achieved, so manufacturers who choose to adopt the core baseline for any of the IoT devices they produce have considerable flexibility in implementing it to effectively address customer needs.

Each row in Table 1 covers one of the device cybersecurity capabilities in the core baseline:

- The first column defines the capability. Note that Figure 3, which is located immediately after Table 1, indicates how the capability relates to the risk mitigation areas and challenges defined in NIST IR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [4].
- The second column provides a numbered list of *key elements* of that capability—elements an IoT device manufacturer seeking to implement the core baseline often (but not always) would use in order to achieve the capability. (Note: the elements are not intended to be comprehensive, nor are they in any particular order.)
- The last column lists IoT reference examples that indicate existing sources of IoT device cybersecurity guidance specifying a similar or related capability. Because the table only covers the basics of the capabilities, the references can be invaluable for understanding each capability in more detail and learning how to implement each capability in a reasonable manner. The following are the references used in Table 1:
    - **AGELIGHT**: AgeLight Digital Trust Advisory Group, "IoT Safety Architecture & Risk Toolkit (IoTSA) v3.1" [10]

[3] The usage of the term "baseline" in this document should not be confused with the low-, moderate-, and high-impact control baselines set forth in NIST Special Publication (SP) 800-53 [5] to help federal agencies meet their obligations under the Federal Information Security Modernization Act (FISMA) and other federal policies. In this document, "baseline" is used in the generic sense to refer to a set of foundational requirements or recommendations.

- **BITAG**: Broadband Internet Technical Advisory Group (BITAG), "Internet of Things (IoT) Security and Privacy Recommendations" [11]
- **CSA**: Cloud Security Alliance (CSA) IoT Working Group, "Identity and Access Management for the Internet of Things" [12]
- **CSDE**: Council to Secure the Digital Economy (CSDE), "The C2 Consensus on IoT Device Security Baseline Capabilities" [13]
- **CTIA**: CTIA, "CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.0.1" [14]
- **ENISA**: European Union Agency for Network and Information Security (ENISA), "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures" [15]
- **ETSI**: European Telecommunications Standards Institute (ETSI), "Cyber Security for Consumer Internet of Things" [16]
- **GSMA**: Groupe Spéciale Mobile Association (GSMA), "GSMA IoT Security Assessment" [17]
- **IEC**: International Electrotechnical Commission (IEC), "IEC 62443-4-2, Edition 1.0, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components" [18]
- **IIC**: Industrial Internet Consortium (IIC), "Industrial Internet of Things Volume G4: Security Framework" [19]
- **IoTSF**: IoT Security Foundation (IoTSF), "IoT Security Compliance Framework, Release 2" [20]
- **ISOC/OTA**: Internet Society/Online Trust Alliance (OTA), "IoT Security & Privacy Trust Framework v2.5" [21]
- **PSA**: Platform Security Architecture (PSA) Joint Stakeholder Agreement (JSA) Members, "PSA Certified™ Level I Questionnaire, Version 1.2" [22]

Table 1: The Core Device Cybersecurity Capability Baseline for Securable IoT Devices

Device Cybersecurity Capability	Key Elements	IoT Reference Examples
Device Identification: The IoT device can be uniquely identified logically and physically.	1. A unique logical identifier 2. A unique physical identifier at an external or internal location on the device authorized entities can access Note: the physical and logical identifiers may represent the same value, but they do not have to.	• **CSA:** 1 • **CSDE**: 5.1.1 • **CTIA**: 4.13 • **ENISA**: GP-PS-10 • **GSMA**: CLP13_6.6.2, 6.8.1, 6.20.1 • **IEC**: CR 1.2 • **IIC**: 7.3, 8.5, 11.7, 11.8 • **IoTSF**: 2.4.8.1, 2.4.14.3, 2.4.14.4 • **PSA:** R2.1
Device Configuration: The configuration of the IoT device's software and firmware can be changed, and such changes can be performed by authorized entities only.	1. The ability to change the device's software and firmware configuration settings 2. The ability to restrict configuration changes to authorized entities only 3. The ability for authorized entities to restore the device to a secure configuration defined by an authorized entity	• **BITAG**: 7.1 • **CSA**: 22 • **ENISA**: GP-TM-06 • **IEC**: CR 7.4, CR 7.6 • **IIC**: 7.3, 7.6, 8.10, 11.5 • **IoTSF**: 2.4.8.17, 2.4.15 • **ISOC/OTA**: 26

- An *authorized entity* is an entity (defined below) that has implicitly or explicitly been granted approval to interact with a particular IoT device. The device cybersecurity capabilities in the core baseline do not specify how authorization is implemented for distinguishing authorized and unauthorized entities. It is left to the manufacturer to decide how each device will implement authorization. Also, an entity authorized to interact with an IoT device in one way might not be authorized to interact with the same device in another way.
- *Configuration* is "the possible conditions, parameters, and specifications with which an information system or system component can be described or arranged." [23] The Device Configuration capability does not define which configuration settings should exist, simply that a mechanism to manage configuration settings exists.
- A *device identifier* is a context-unique value—a value unique within a specific context—that is associated with a device (for example, a string consisting of a network address). (This definition is derived from [24].)
- An *entity* is a person, device, service, network, domain, manufacturer, or other party who might interact with an IoT device.
- *Firmware* is "software that is included in read-only memory (ROM)." [25]
- A *logical identifier* is a device identifier that is expressed logically by the device's software or firmware. An example is a media access control (MAC) address assigned to a network interface.
- A *physical identifier* is a device identifier that is expressed physically by the device (e.g., printed onto a device's housing, displayed on a device's screen).
- *Software* is "computer programs and associated data that may be dynamically written or modified during execution." [5]

Device Cybersecurity Capability	Key Elements	IoT Reference Examples
Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.	1. The ability to use demonstrably secure cryptographic modules for standardized cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of the device's stored and transmitted data from being compromised 2. The ability for authorized entities to render all data on the device inaccessible by all entities, whether previously authorized or not (e.g., through a wipe of internal storage, destruction of cryptographic keys for encrypted data) 3. Configuration settings for use with the **Device Configuration** capability including, but not limited to, the ability for authorized entities to configure the cryptography use itself, such as choosing a key length	• **AGELIGHT**: 5, 7, 18, 24, 25, 34 • **BITAG**: 7.2, 7.10 • **CSDE**: 5.1.3, 5.1.4, 5.1.5, 5.1.8, 5.1.10 • **CTIA**: 4.8, 5.14, 5.15 • **ENISA**: GP-OP-04, GP-TM-02, GP-TM-04, GP-TM-14, GP-TM-24, GP-TM-32, GP-TM-34, GP-TM-35, GP-TM-39, GP-TM-40 • **ETSI**: 4.4-1, 4.5-1, 4.5-2, 4.11-1, 4.11-2, 4.11-3 • **GSMA:** CLP13_6.4.1.1, 6.11, 6.12.1.1, 6.19, 7.6.1, 8.10.1.1, 8.11.1 • **IEC**: CR 3.1, CR 3.4, CR 4.1, CR 4.2, CR 4.3 • **IIC**: 7.3, 7.4, 7.6, 7.7, 8.8, 8.11, 8.13, 9.1, 10.4, 11.9 • **IoTSF**: 2.4.6.5, 2.4.7, 2.4.8.8, 2.4.8.16, 2.4.9, 2.4.12.2, 2.4.16.1, 2.4.16.2 • **ISOC/OTA**: 2, 17, 33 • **PSA:** C1.4, C2.4, D2.3, D2.4, D3.1, D4.5, D5.1, D5.2, R2.2, R2.3, R3.2, R3.3, R6.1
Logical Access to Interfaces: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.	1. The ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device 2. The ability to logically restrict access to each network interface (e.g., device authentication, user authentication) 3. Configuration settings for use with the **Device Configuration** capability including, but not limited to, the ability to enable, disable, and adjust thresholds for any ability the device might have to lock or disable an account or to delay additional authentication attempts after too many failed authentication attempts	• **AGELIGHT**: 10, 13, 14, 15, 16, 19 • **BITAG**: 7.1, 7.2, 7.3, 7.6 • **CSA:** 2, 4, 20 • **CSDE**: 5.1.2 • **CTIA**: 3.2, 3.3, 3.4, 4.2, 4.3, 4.9, 5.2 • **ENISA**: GP-TM-08, GP-TM-09, GP-TM-21, GP-TM-22, GP-TM-25, GP-TM-27, GP-TM-29, GP-TM-33, GP-TM-42, GP-TM-44, GP-TM-45 • **ETSI**: 4.1-1, 4.4-1, 4.6-1, 4.6-2 • **GSMA**: CLP13_6.9.1, 6.12.1, 6.20.1, 7.6.1, 8.2.1, 8.4.1 • **IEC**: CR 1.1, CR 1.2, CR 1.5, CR 1.7, CR 1.11, CR 2.1, CR 2.2, CR 2.13, CR 7.7, EDR 2.13 • **IIC**: 7.3, 7.4, 8.3, 8.6, 11.7 • **IoTSF**: 2.4.4.5, 2.4.4.9, 2.4.5.5, 2.4.6.3, 2.4.6.4, 2.4.7, 2.4.8 • **ISOC/OTA**: 3, 12, 13, 14, 15, 16 • **PSA:** C2.3, D2.1, D2.2, D3.3, D4.1, D4.2, D4.3, R3.1, R4.2, R5.1, R5.2

- An *interface* is a boundary between the IoT device and entities where interactions take place. (This definition is derived from [26].) There are two types of interfaces: network and local.
- *Local interfaces* are interfaces that can only be accessed physically, such as ports (e.g., USB, audio, video/display, serial, parallel, Thunderbolt) and removable media drives (e.g., CD/DVD drives, memory card slots).
- *Network interfaces* are interfaces that connect the IoT device to networks.

Device Cybersecurity Capability	Key Elements	IoT Reference Examples
Software and Firmware Update: The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.	1. The ability to update the device's software and firmware through remote (e.g., network download) and/or local means (e.g., removable media) 2. The ability to confirm the validity of any update before installing it 3. The ability for authorized entities to roll back updated software and firmware to a previous version 4. The ability to restrict updating actions to authorized entities only 5. The ability to enable or disable updating 6. Configuration settings for use with the **Device Configuration** capability including, but not limited to: a. The ability to configure remote update mechanisms to be either automatically or manually initiated for update downloads and installations b. The ability to enable or disable notification when an update is available and specify who or what is to be notified	• **AGELIGHT**: 1, 2, 4 • **BITAG**: 7.1 • **CSDE**: 5.1.9 • **CTIA**: 3.5, 3.6, 4.5, 4.6, 5.5, 5.6 • **ENISA**: GP-TM-05, GP-TM-06, GP-TM-18, GP-TM-19 • **ETSI**: 4.3-1, 4.3-2, 4.3-7 • **GSMA**: 7.5.1 • **IEC**: CR 3.4, EDR 3.10 • **IIC**: 7.3, 11.5.1 • **IoTSF**: 2.4.5.1, 2.4.5.2, 2.4.5.3, 2.4.5.4, 2.4.5.8, 2.4.6.1 • **ISOC/OTA**: 1, 6, 8 • **PSA:** C2.1, C2.2, R1.1, R1.2
Cybersecurity State Awareness: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.	1. The ability to report the device's cybersecurity state 2. The ability to differentiate between when a device will likely operate as expected from when it may be in a degraded cybersecurity state 3. The ability to restrict access to the state indicator so only authorized entities can view it 4. The ability to prevent any entities (authorized or unauthorized) from editing the state except for the device's monitor 5. The ability to make the state information available to a service on another device, such as an event/state log server	• **CSDE**: 5.1.7 • **CTIA**: 4.7, 4.12, 5.7, 5.16 • **ENISA**: GP-TM-55, GP-TM-56 • **ETSI**: 4.7-2, 4.10-1 • **GSMA**: CLP13_6.13.1, 7.2.1, 9.1.1.2 • **IEC**: CR 2.8, CR 3.9, CR 6.1, CR 6.2 • **IIC**: 7.3, 7.5, 7.7, 8.9, 10.3, 10.4 • **IoTSF**: 2.4.7.5 • **PSA**: D3.2, D3.4, R4.1, R4.3

- A *cybersecurity state* is the condition of a device's cybersecurity expressed in a way that is meaningful and useful to the device's customer. For example, a very simple device might express its state in terms of whether or not it is operating as expected, while a complex device might perform cybersecurity logging, check its integrity at boot, and examine and report additional aspects of its cybersecurity state.
- A *degraded cybersecurity state* is a cybersecurity state that indicates the device's cybersecurity has been significantly negatively impacted, such as the device being unable to operate as expected, or the integrity of the device's firmware being violated.
- An *update* is a patch, upgrade, or other modification to code that corrects security and/or functionality problems in software or firmware. (This definition is derived from [27].)

Manufacturers should keep in mind that the capabilities presented in Table 1 are meant as a starting point to help provide the means customers may need to apply common risk mitigations. Figure 3 below shows the risk mitigation area and challenges defined in NIST IR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [4] that would be supported, in part, by the core capabilities defined in Table 1.

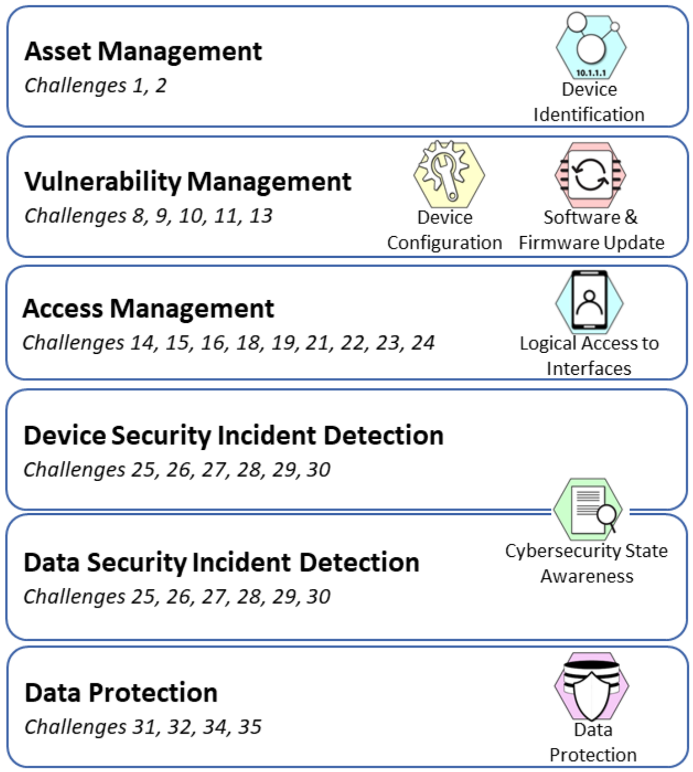

Figure 3: NISTIR 8228 Risk Mitigation Areas Supported by Each Core Device Cybersecurity Capability

3.4 Activity 4: Plan for Adequate Support of Customer Goals

It is important for manufacturers to consider how to support their customers' goals once they are identified, including provisioning of computing resources to support device cybersecurity capabilities, as well as actions external to the device that may be required to continue to support cybersecurity goals.

Manufacturers can help make their IoT devices more securable by appropriately provisioning device hardware resources (e.g., processing, memory, storage, network technology, power), as well as firmware and software resources, to support the desired device cybersecurity capabilities. For example, software-based encryption is processing-intensive, and a device with limited processing and no hardware-based encryption might not be able to provide what customers need. Another example is that some devices cannot support the use of an operating system or Internet Protocol (IP) networks, and one or both of those might be needed to support multiple device cybersecurity capabilities.

When designing or selecting device hardware, firmware, and software resources, manufacturers can answer the following questions for the expected customers and use cases to help identify provisioning needs and potential issues:

1. **What potential future use needs to be taken into account?** For example, if a device has a 10-year lifespan, it may be necessary to update the encryption algorithm or key length the device uses during that time, and the new algorithm or key length may require more processing resources than the current algorithm or key length does.
2. **Should an established IoT platform be used instead of acquiring and integrating individual hardware, firmware, and software components?** An *IoT platform* is a piece of IoT device hardware with firmware and/or supporting software already installed and configured for a manufacturer's use as the basis of a new IoT device. An IoT platform might also offer third-party services or applications, or a software development kit (SDK) to help expedite IoT application development. Manufacturers can choose a sufficiently resourced and adequately secure IoT platform instead of designing hardware, installing and configuring an operating system or firmware, creating new cloud-based services, writing IoT device applications and mobile apps from scratch, and performing other tasks that are error-prone and generally more likely to introduce new vulnerabilities into the IoT device compared to adopting an established platform.
3. **Should any of the device cybersecurity capabilities be hardware-based?** An example is having a hardware root of trust that provides trusted storage for cryptographic keys and enables performing secure boots and confirming device authenticity. Note that for some device cybersecurity capabilities, providing them in hardware could reduce agility for meeting future needs.
4. **Does the hardware, firmware, or software (including the operating system) include unneeded device capabilities with cybersecurity implications? If so, can they be disabled to prevent misuse and exploitation?** For example, a device may have local interfaces on its external housing that are useful for some or future expected use cases, but the device may be deployed in public areas by some expected customers, where those interfaces would be exposed to possible attack. Possible approaches to this issue include offering a tamper-resistant enclosure to prevent physical access to the interfaces, and offering a configuration option that logically disables the interfaces.

Manufacturers should consider which, if any, secure development practices are most appropriate for them and their customers as they further plan how to adequately support customer goals. Manufacturers can answer questions like the following based on expected customers and uses cases to help identify additional action to take towards cybersecurity:

1. **How is IoT device code protected from unauthorized access and tampering?** (e.g., well-secured code repository, version control features, code signing)
2. **How can customers verify software integrity for the IoT device?** (e.g., code signature validation, cryptographic hash comparison)
3. **What verification is done to confirm that the security of third-party software used within the IoT device meets the customers' needs?** (e.g., check for known

vulnerabilities that are not yet fixed, review or analyze human-readable code, test executable code)

4. **What measures are taken to minimize the vulnerabilities in released IoT device software?** (e.g., follow secure coding practices, review and analyze human-readable code, test executable code, configure software to have secure settings by default)

5. **What measures are taken to accept reports of possible IoT device software vulnerabilities and respond to them?** (e.g., vulnerability response program, vulnerability database monitoring, threat intelligence service use)

6. **What processes are in place to assess and prioritize the remediation of all vulnerabilities in IoT device software?** (e.g., estimate remediation effort, estimate potential impact of exploitation, estimate attacker resources needed to weaponize the vulnerability)

IoT device manufacturers interested in more information on secure software development practices can consult the NIST white paper *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)* [28], which highlights selected practices for secure software development. Each of these practices is widely recommended by existing secure software development publications, and the white paper provides references from nearly 20 of these publications.

4 Manufacturer Activities Impacting the IoT Device Post-Market Phase

Manufacturers of IoT devices will at some point market and sell their product, which will put it in the hands of customers and initiate the manufacturing post-market phase. While customers are evaluating potential product acquisitions, and after those products are sold to customers, manufacturers continue to have a role in supporting the customers' cybersecurity goals and the IoT devices, such as responding to vulnerability reports, and producing and disseminating updates. These activities can benefit customers and their ability to secure devices throughout their life, particularly as they assess and acquire IoT devices available on the market.

Though this section aims to help securability by making it easier for customers to understand and identify how IoT devices are built to meet their cybersecurity expectations, which will primarily impact post-market activities, planning for these activities (e.g., answering the presented questions for each activity) is best performed before an IoT is marketed and sold to customers. This planning should occur when information needed becomes available through various pre-market activities, such as those discussed in Section 3. Though Activities 1 through 4 may help inform planning and execution of the activities presented in this section, they are not considered a prerequisite. This allows some or all aspects of the planning for Activities 5 and 6 to happen in parallel with other pre-market activities.

An often-overlooked aspect of both marketing and the post-market phase is communication related to cybersecurity. Many customers will benefit from manufacturers communicating to them—or others acting on the customers' behalf—more clearly about cybersecurity risks involving the IoT devices the manufacturers are currently selling or have already sold. This section describes two broad activities related to customer communications that manufacturers should consider performing to improve how securable their IoT devices are for customers after they are sold. The considerations mentioned within these activities may not apply to all customers or manufacturers, but others may find the same considerations to be vital. Even if adopted, the outcomes of these activities will take different forms as many methods can be used to achieve the describe outcomes, and different methods may be needed for different kinds of customers.

4.1 Activity 5: Define Approaches for Communicating to Customers

Clearly communicating cybersecurity information may necessitate different communication approaches for different kinds of customers based on their expectations and resources. Manufacturers can answer questions like the following to help define communication approaches:

1. **What terminology will the customer understand?** For example, a home user will likely have less technical knowledge than points of contact at a large business (e.g., system administrators). Also, IT and cybersecurity professionals may already be familiar with conventions like referring to a vulnerability by its Common Vulnerabilities and Exposures (CVE) number.

2. **How much information will the customer need?** Giving a customer too much information may overwhelm them and make it harder for them to find the information they need. Not providing enough information is generally undesirable, except for cases

where revealing the information might have broader negative implications—for example, publishing technical details of a newly discovered vulnerability before an update is available to correct the vulnerability.

3. **How/where will the information be provided?** Information can be provided in one or more logical and/or physical locations. Examples include user manuals and other product documentation, websites, emails, and the IoT device itself and its associated applications (e.g., mobile apps). Customers will benefit more when they can readily locate information whenever needed.
4. **How can the integrity of the information be verified?** For some methods of providing information, such as emails, customers may want a way to determine if the information is legitimate (e.g., not a social engineering attempt).

4.2 Activity 6: Decide What to Communicate to Customers and How to Communicate It

There are many potential considerations for what information a manufacturer communicates to customers for a particular IoT product and how that information will be communicated. The rest of this section contains examples of topics that manufacturers might want to include in their communications and, for some examples, thoughts on how that information might be communicated.

4.2.1 Cybersecurity Risk-Related Assumptions

To understand how their risk might differ from the manufacturer's expectations, some customers may benefit by knowing the cybersecurity-related assumptions the manufacturer made when designing and developing the device, such as the following:

1. **Who were the expected customers?** For example, some IoT devices are created with a specific sector or customer type in mind, which could impact not only which device cybersecurity capabilities are implemented, but also how those capabilities function, which may not be how all customers expect.
2. **How was the device intended to be used?** For example, some IoT devices have specific intended purposes in systems, which may drive cybersecurity considerations for customers.
3. **What types of environment would the device be used in?** Customers may need to know, for example, if an IoT device may not be securable if in a public location or without the use of another device that provides some or all device cybersecurity capabilities on behalf of the IoT device.
4. **How would responsibilities be shared among the manufacturer, the customer, and others?** For example, some customers may benefit from knowing if device cybersecurity capabilities and tasks such as software and firmware updates, device configuration, data protection and destruction, and device management may be performed by one party or multiple parties.

4.2.2 Support and Lifespan Expectations

Communicating device support and lifespan expectations helps customers plan their cybersecurity risk mitigations throughout the device's support lifecycle, which may be shorter than how long the customer wants to use the device. To determine what information to communicate to customers, manufacturers can answer questions like the following:

1. **How long do you intend to support the device?** For example, telling customers how long updates and technical support will be available may help them plan to securely use and maintain devices for an appropriate amount of time.
2. **When do you intend for device end-of-life to occur?** For example, customers may want to plan to retire a device when the manufacturer considers the device at end-of-life.
3. **What functionality, if any, will the device have after support ends and at end-of-life?** For example, customers may want to know if they will be able to continue use of a device at its end-of-life, even if cloud-based services or other functions are no longer available.
4. **How can customers report suspected problems with cybersecurity implications, such as software vulnerabilities, to the manufacturer? Will reports be accepted after support ends? Will reports be accepted after end-of-life?** Examples of reporting methods include phone numbers, email addresses, and web forms.

4.2.3 Technical and Non-Technical Means

Communicating information about the device cybersecurity capabilities the device provides (technical means within the device), as well as the technical means that can be provided by a related device or a manufacturer service or system, helps customers better understand how to manage risk for the device. To determine what information about device cybersecurity capabilities is important to communicate to customers, manufacturers can answer questions like the following:

1. **Which technical means can be provided**
    a. **by the device itself (device cybersecurity capabilities)?** Examples include encryption used by the device for data protection, the presence of a physical identifier on the device, and authentication and authorization mechanisms the device uses to limit access to its network interfaces.
    b. **by a related device?** For example, some technical means may be delivered or supported by an IoT hub or mobile device the IoT device is associated with.
    c. **by a manufacturer service or system?** An example would be technical means provided by an internet server or cloud-hosted service.
2. **Which technical or non-technical means should the customer provide themselves or consider providing themselves?** An example is using network-based security controls to prevent direct access to the device from the internet, such as a firewall.
3. **How is each of the technical and non-technical means expected to affect cybersecurity risk?** For example, proper implementation of data protection may help mitigate confidentiality risks, but may also reduce availability (e.g., if data cannot be decrypted or is decrypted slowly), which could worsen availability risks.

4.2.4 Device Composition and Capabilities

Communicating information about the device's software, firmware, hardware, services, functions, and data types helps customers better understand and manage cybersecurity for their devices, particularly if the customer is expected to play a substantial role in managing device cybersecurity. To determine what information is important to communicate to customers, manufacturers can answer questions like the following:

1. **What information do customers need on general cybersecurity-related aspects of the device, including device installation, configuration (including hardening), usage, management, maintenance, and disposal?** Examples include how the device can securely join a system, what aspects of configuration may impact cybersecurity, and what ways of using the device are known to be insecure.

2. **What is the potential effect on the device if the cybersecurity configuration is made more restrictive than the secure default?** For example, some devices may lose some functionality as their cybersecurity configurations are made more stringent.

3. **What inventory-related information do customers need for the device's internal software and firmware, such as versions, patch status, and known vulnerabilities? Do customers need to be able to access the current inventory on demand?** For example, some customers may want to be aware of known vulnerabilities so they can address them through other means, while other customers may want to know the current software and firmware patch levels.

4. **What information do customers need about the sources of the device's software, firmware, hardware, and services?** Examples of sources include the developer of the device's IoT software, the manufacturer of the device's processor, and the provider of a cloud-based service used by the device.

5. **What information do customers need on the device's operational characteristics so they can adequately secure the device? How should this information be made available?** For example, some customers may be best served by placing the information on a website, while others may make best use of the information through a standardized machine-to-machine protocol.

6. **What functions can the device perform?** This includes not only device cybersecurity capabilities, but also any other functions that may have cybersecurity implications—for example, transmitting data to a remote system, or using a microphone and camera to capture audio and video.

7. **What data types can the device collect? What are the identities of all parties (including the manufacturer) that can access that data?** For example, some customers may need to know if location information or voice commands collected by the device may be stored in a cloud and accessed for aggregation or analytics.

8. **What are the identities of all parties (including the manufacturer) who have access to or any degree of control over the device?** For example, a third party providing technical support on behalf of the manufacturer might be able to remotely update the device's software and configuration.

4.2.5 Software and Firmware Updates

Manufacturers communicating information about updates helps customers plan their cybersecurity risk mitigations and maintain the cybersecurity of their devices, particularly in response to emerging threats. To determine what update information is important to communicate to customers, manufacturers can answer questions like the following:

1. **Will updates be made available? If so, when will they be released?** For example, knowing if updates will be provided on a set schedule or sporadically will help customers plan for applying them.
2. **Under what circumstances will updates be issued?** Examples include controlling the execution of faulty software and correcting a previously unknown vulnerability in a standard protocol.
3. **Which entity (e.g., customer, manufacturer, third party) is responsible for performing updates? Or can the customer designate which entity will be responsible?** For example, some customers may benefit from knowing that firmware updates will be available from a third party and software updates will be provided by the manufacturer. Some customers may likewise benefit from being made aware of their roles, responsibilities, and options around updates.
4. **How can customers verify and authenticate updates?** Examples are cryptographic hash comparison, code signature validation, and reliance on manufacturer-provided software that automatically performs update verification and authentication.
5. **What information should be communicated with each individual update?** Examples are the nature of the update (e.g., corrections to errors, altered or new capabilities) and any effect installing the update could have on a customer's existing configuration settings.

4.2.6 Device Retirement Options

Manufacturers communicating information about device retirement options helps customers plan for doing so securely. To determine what update information is important to communicate to customers, manufacturers can answer questions like the following:

1. **Will customers want to transfer ownership of their devices to another party? If so, what do customers need to do so their user and configuration data on the device and associated systems (e.g., cloud-based services used by the device) are not accessible by the party who assumes ownership?** For example, a customer may want to sell a building that contains smart building automation devices, but would want a way to ensure all data has been removed from the devices before the building buyer gains access to them.
2. **Will customers want to render their devices inoperable? If so, how can customers do that?** For example, some IoT devices can be rendered inoperable through logical means (e.g., as executed through a mobile app), while others use physical means (e.g., a button on the device).

5 Next Steps for Manufacturers

Sections 3 and 4 define six cybersecurity-related activities for IoT device manufacturers and give examples of questions manufacturers can answer for each activity. Manufacturers who choose to perform an activity should determine the applicability of the example questions and identify any other questions that may help to understand customers' cybersecurity goals and the means the customers expect, then answer the questions.

As Figure 4 conceptually depicts, IoT device manufacturers can use a variety of sources to gather the information they need to answer the questions. In some instances, expected customers and use cases will point to existing laws, regulations, or voluntary guidance for cybersecurity and other aspects of device operation. For example, IoT devices intended to be used by the federal government would be secured using security controls derived from guidance that is considered by agencies for securing the systems that would include IoT devices (e.g., NIST SP 800-53 [5], Cybersecurity Framework [6]). For some use cases, guidance may go beyond cybersecurity risks but will still have direct or indirect implications for cybersecurity, such as devices in the medical sector needing to comply with Food and Drug Administration (FDA) regulations and the Health Insurance Portability and Accountability Act (HIPAA). Many industrial sectors will also have consensus and/or voluntary guidance that is expected to be followed by their stakeholders.

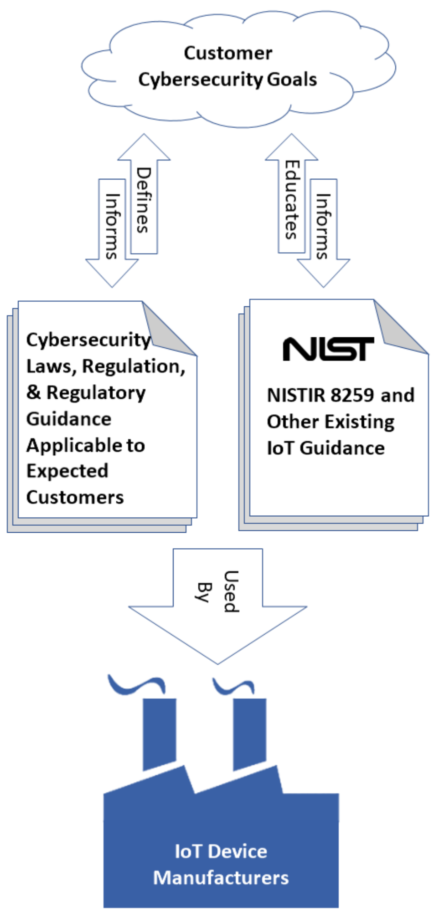

Figure 4: Customer Cybersecurity Goals Informed and Reflected by Many Sources Manufacturers Can Use

For some customers or sectors, such explicit written guidance may not be readily available or usable (e.g., due to high variability in goals for customers within a sector). For devices intended to be used by these customers, ascertaining their goals may require use of other forms of information, such as gathering information directly from customers or conducting secondary research to gain a better understanding of their goals. With this information, manufacturers can follow a process of linking cybersecurity mitigation goals with specific device cybersecurity capabilities, as was used to make the core baseline, to determine the common device cybersecurity capabilities needed by many of their customers. Manufacturers can then implement these capabilities within their IoT devices to help as many customers achieve as many of their goals as is feasible. Other baselines building upon the core presented in this document can further help manufacturers identify device cybersecurity capabilities expected by customers. Figure 5 shows how additional baselines, as well as how specific, niche cybersecurity needs, such as those for a vertical within a sector, may adapt from and build upon each other.

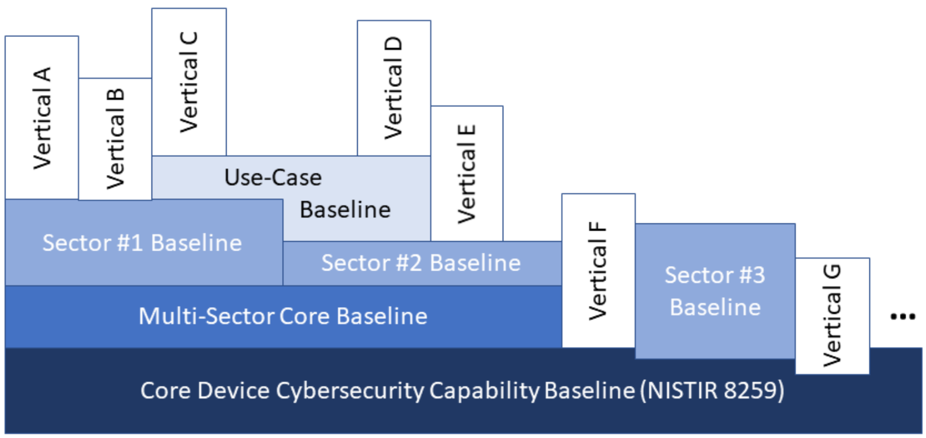

Figure 5: How Additional Device Cybersecurity Capabilities Could Build Upon the Core Baseline

1021 # References

[1] Simmon E (forthcoming) A Model for the Internet of Things (IoT). (National Institute of Standards and Technology, Gaithersburg, MD).

[2] Executive Order no. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, DCPD-201700327, May 11, 2017. https://www.govinfo.gov/app/details/DCPD-201700327

[3] Department of Commerce (2018) A Road Map Toward Resilience Against Botnets. (Department of Commerce, Washington, DC). https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_0.pdf

[4] Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas K, Nadeau E, Piccarreta B, Gabel O'Rourke D, Scarfone K (2019) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8228. https://doi.org/10.6028/NIST.IR.8228

[5] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[6] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[7] Stouffer K, Pillitteri V, Lightman S, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev 2. https://doi.org/10.6028/NIST.SP.800-82r2

[8] Cyber-Physical Systems Public Working Group (2017) Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1500-201. https://doi.org/10.6028/NIST.SP.1500-201

[9] Merriam-Webster (2017) Webster's Third New International Dictionary Unabridged. (Merriam-Webster, Springfield, MA).

[10] AgeLight Digital Trust Advisory Group (2019) IoT Safety Architecture & Risk Toolkit (IoTSA) v3.1. (AgeLight Advisory & Research Group, Bellevue, WA). http://agelight.com/iot.html

[11] Broadband Internet Technical Advisory Group (BITAG) (2016) Internet of Things (IoT) Security and Privacy Recommendations. (Broadband Internet Technical Advisory Group [BITAG], Denver, CO). https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[12] Cloud Security Alliance (CSA) IoT Working Group (2015) Identity and Access Management for the Internet of Things. (Cloud Security Alliance [CSA]). https://cloudsecurityalliance.org/download/identity-and-access-management-for-the-iot/

[13] Council to Secure the Digital Economy (CSDE) (2019) The C2 Consensus on IoT Device Security Baseline Capabilities. (Council to Secure the Digital Economy [CSDE]). https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

[14] CTIA (2018) CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.0.1. (CTIA, Washington, DC). https://www.ctia.org/about-ctia/test-plans/

[15] European Union Agency for Network and Information Security (ENISA) (2017) Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. (European Union Agency for Network and Information Security [ENISA], Athens, Greece). https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[16] European Telecommunications Standards Institute (ETSI) (2019) Cyber Security for Consumer Internet of Things. ETSI Technical Specification 103 645 V1.1.1.[4] (European Telecommunications Standards Institute [ETSI], Sophia Antipolis Cedex, France). https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

[17] Groupe Spéciale Mobile Association (GSMA) (2017) GSMA IoT Security Assessment. (Groupe Spéciale Mobile Association [GSMA], London, UK). https://www.gsma.com/iot/iot-security-assessment/

[18] International Electrotechnical Commission (IEC) (2019) IEC 62443-4-2, Edition 1.0, Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components. (International Electrotechnical Commission [IEC], Geneva, Switzerland). https://webstore.iec.ch/publication/34421

[19] Industrial Internet Consortium (IIC) (2016) Industrial Internet of Things Volume G4: Security Framework. (Industrial Internet Consortium [IIC], Needham, MA). https://www.iiconsortium.org/IISF.htm

[20] IoT Security Foundation (IoTSF) (2018) IoT Security Compliance Framework, Release 2. (IoT Security Foundation [IoTSF], Livingston, Scotland). https://www.iotsecurityfoundation.org/best-practice-guidelines/

[21] Online Trust Alliance (OTA) (2017) IoT Security & Privacy Trust Framework v2.5. (Online Trust Alliance [OTA], an Internet Society initiative). https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/

[22] Platform Security Architecture (PSA) Joint Stakeholder Agreement (JSA) Members (2019) PSA Certified™ Level 1 Questionnaire, Version 1.2. (Arm Limited, Cambridge, United Kingdom). https://www.psacertified.org/security-certification/psa-certified-level-1

[23] Johnson A, Dempsey K, Ross R, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128. https://doi.org/10.6028/NIST.SP.800-128

[4] ETSI is currently developing ETSI European Standard 303 645, which is similar to but not identical to the 103 645 Technical Specification cited here. The 303 645 version is not used in this publication because it is still a draft.

[24] Barker E, Chen L, Roginsky A, Vassilev A, Davis R (2019) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-56A, Rev. 3. https://doi.org/10.6028/NIST.SP.800-56Ar3

[25] Cooper D, Polk W, Regenscheid A, Souppaya M (2011) BIOS Protection Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-147. https://doi.org/10.6028/NIST.SP.800-147

[26] Committee on National Security Systems (2015) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Ft. Meade, MD), CNSS Instruction (CNSSI) No. 4009.

[27] Souppaya M, Scarfone K (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3. https://doi.org/10.6028/NIST.SP.800-40r3

[28] Dodson D, Souppaya M, Scarfone K (2019) Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF). (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Cybersecurity White Paper. https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf

Appendix A—Acronyms and Abbreviations

Selected acronyms and abbreviations used in this document are defined below.

BITAG	Broadband Internet Technical Advisory Group
CD	Compact Disc
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CSA	Cloud Security Alliance
CSDE	Council to Secure the Digital Economy
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DVD	Digital Video Disc
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
GSMA	Groupe Spéciale Mobile Association
IACS	Industrial Automation and Control Systems
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IIC	Industrial Internet Consortium
IoT	Internet of Things
IoTSA	Internet of Things Safety Architecture & Risk Toolkit
IoTSF	Internet of Things Security Foundation
IP	Internet Protocol
IR	Internal Report
IT	Information Technology
ITL	Information Technology Laboratory
LTE	Long-Term Evolution
MAC	Media Access Control
NIST	National Institute of Standards and Technology
OTA	Online Trust Alliance
PII	Personally Identifiable Information
ROM	Read-Only Memory
SDK	Software Development Kit
SP	Special Publication
SSDF	Secure Software Development Framework
USB	Universal Serial Bus
UWB	Ultra-Wideband
Wi-Fi	Wireless Fidelity

Appendix B—Glossary

Selected terms used in this document are defined below.

Actuator	A portion of an IoT device capable of changing something in the physical world. [4]
Authorized Entity	An entity that has implicitly or explicitly been granted approval to interact with a particular IoT device.
Configuration	"The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged." [23]
Core Baseline	A set of technical device capabilities needed to support common cybersecurity controls that protect the customer's devices and device data, systems, and ecosystems.
Core Device Cybersecurity Capability Baseline	See *core baseline*.
Cybersecurity State	The condition of a device's cybersecurity expressed in a way that is meaningful and useful to the device's customer.
Degraded Cybersecurity State	A cybersecurity state that indicates the device's cybersecurity has been significantly negatively impacted.
Device Cybersecurity Capability	A cybersecurity feature or function provided by an IoT device through its own technical means (i.e., device hardware, firmware, and software).
Device Identifier	A context-unique value—a value unique within a specific context—that is associated with a device (for example, a string consisting of a network address). (derived from [24])
Entity	A person, device, service, network, domain, manufacturer, or other party who might interact with an IoT device.
Firmware	"Software that is included in read-only memory (ROM)." [25]
Interface	A boundary between the IoT device and entities where interactions take place. (derived from [26])
IoT Platform	A piece of IoT device hardware with firmware and/or supporting software already installed and configured for a manufacturer's use as the basis of a new IoT device. An IoT platform might also offer third-party services or applications, or a software development kit to help expedite IoT application development.
Local Interface	An interface of an IoT device that can only be accessed physically, such as a port or a removable media drive.

Logical Identifier	A device identifier that is expressed logically by the device's software or firmware.
Means	"An agent, tool, device, measure, plan, or policy for accomplishing or furthering a purpose." [9]
Minimally Securable IoT Device	An IoT device that has the device cybersecurity capabilities (i.e., hardware, firmware, and software) customers may need to implement cybersecurity controls used to mitigate some common cybersecurity risks.
Network Interface	An interface that connects an IoT device to a network (e.g., Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution [LTE], Zigbee, Ultra-Wideband [UWB]).
Physical Identifier	A device identifier that is expressed physically by the device (e.g., printed onto a device's housing, displayed on a device's screen).
Remote Logical Access	Logical access to an IoT device that occurs over a network.
Sensor	A portion of an IoT device capable of providing an observation of an aspect of the physical world in the form of measurement data. [4]
Software	"Computer programs and associated data that may be dynamically written or modified during execution." [5]
Transducer	A portion of an IoT device capable of interacting directly with a physical entity of interest. The two types of transducers are sensors and actuators. [4]
Update	A patch, upgrade, or other modification to code that corrects security and/or functionality problems in software or firmware. (derived from [27])